That which is claimed:

1. A method of single sign-on user access to multiple web servers, comprising:

authenticating a user at a first web server;

transmitting an encrypted authentication token from the first web server to a second web server, wherein the authentication token comprises an expiration time and is digitally signed by the first web server;

authenticating the authentication token at the second web server; and

allowing the user to conduct a session at the second web server.

2. The method of claim 1 wherein the first web server and the second web server share a sub-domain.

3. The method of claim 2 further comprising examining the expiration time of the authentication token at the second web server and allowing the user to conduct a session at the second web server only if the expiration time has not passed.

4. The method of claim 3 wherein the authentication token comprises a cookie.

5. The method of claim 4 wherein transmitting the encrypted authentication token from the first web server to the second web server comprises transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server.

6. The method of claim 5 wherein authenticating the user at the first web server comprises receiving a user name and password.

7. The method of claim 6 wherein transmitting the encrypted authentication token from the first web server to a second web server comprises transmitting the authentication token from the first web server to a computer of the user; and transmitting the authentication token from the computer of the user to the second web server.

8. The method of claim 7 wherein the first web server and the second web server comprise a federation of web servers.

9. The method of claim 8 wherein authenticating the authentication token at the second web server comprises examining the cookie.

10. The method of claim 9 further comprising URL encoding the authentication token.

11. The method of claim 10 further comprising URL decoding the authentication token at the second web server.

12. The method of claim 11 further comprising providing a web page to the user having a service selector.

13. The method of claim 12 wherein the service selector comprises a hyperlink.

14. The method of claim 13 wherein the hyperlink comprises a URL for the second web server.

15. A method for single sign-on user access to a federation of web servers, comprising:

allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device;

authenticating the user with user-provided authentication information, including at least a user identification, by the first web server;

prompting the user for selection of a functionality offered via at least a second web server;

receiving a selection by the user of the functionality offered via the second web server;

creating an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server;

digitally signing the authentication token by the first web server;

qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server;

sending the digitally signed authentication token to the web browser of the computing device by the first web server;

redirecting the web browser to the second web server by the first web server;

sending the authentication token to the second web server by the web browser;

decrypting the authentication token by the second web server;

checking the pre-defined expiry of the authentication token by the second web server; and

allowing the user to conduct a session with the second web server if within the pre-defined token expiry.

16. The method of claim 15 further comprising allowing the user to conduct a session with the first web server.

17. The method of claim 16 wherein the second web server shares a sub-domain with the first web server.

18. The method of claim 17 wherein digitally signing the authentication token by the first web server comprising digitally signing the authentication token using public key encryption.

19. The method of claim 18 further comprising confirming a match with the digital signature.

20. A method of single sign-on for multiple web servers, comprising:

receiving log-in data from a user in a first server;

providing the user with a service selector;

receiving an indication that the user selected the service selector;

constructing an authentication token comprising profile data associated with the user;

encrypting and signing the authentication token;

redirecting the user to a second server;

transmitting the authentication token to the user;

receiving the authentication token in the second server;

verifying the authentication token in the second server; and

allowing the user access to a service provided by the second server.

21. The method of claim 20 wherein the authentication token further comprises expiration time data.

22. The method of claim 21 wherein the authentication token comprises a cookie.

23. The method of claim 22 wherein the log-in data comprises a user name and password.

24. The method of claim 23 wherein the service selector comprises a hyperlink.

25. A system for single sign-on user access to multiple web servers, comprising:

a means for authenticating a user at a first web server;

a means for transmitting an encrypted authentication token from the first web server to a second web server, wherein the authentication token comprises an expiration time and is digitally signed by the first web server;

a means for authenticating the authentication token at the second web server; and

a means for allowing the user to conduct a session at the second web server.

26. The system of claim 25 wherein the first web server and the second web server share a sub-domain.

27. The system of claim 26 further comprising a means for examining the expiration time of the authentication token at the second web server.

28. The system of claim 27 wherein the authentication token comprises a cookie.

29. The system of claim 28 wherein the means for transmitting the encrypted authentication token from the first web server to the second web server comprises means for transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server.

30. The system of claim 29 wherein the means for authenticating the user at the first web server comprises means for receiving a user name and password.

31. The system of claim 30 wherein the means for transmitting the encrypted authentication token from the first web server to a second web server comprises means for transmitting the authentication token from the first web server to a computer of the user and means for transmitting the authentication token from the computer of the user to the second web server.

32. The system of claim 31 wherein the first web server and the second web server comprise a federation of web servers.

33. The system of claim 32 wherein the means for authenticating the authentication token at the second web server comprises means for examining the cookie.

34. The system of claim 33 further comprising a means for URL encoding the authentication token.

35. The system of claim 34 further comprising a means for URL decoding the authentication token at the second web server.

36. The system of claim 35 further comprising a means for providing a web page to the user having a service selector.

37. The system of claim 36 wherein the service selector comprises a hyperlink.

38. The system of claim 37 wherein the hyperlink comprises a URL for the second web server.

39. A system for single sign-on user access to a federation of web servers, comprising:

a means for allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device;

a means for authenticating the user with user-provided authentication information, including at least a user identification, by the first web server;

a means for prompting the user for selection of a functionality offered via at least a second web server;

a means for receiving a selection by the user of the functionality offered via the second web server;

a means for creating an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server;

a means for digitally signing the authentication token by the first web server;

a means for qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server;

a means for sending the digitally signed authentication token to the web browser of the computing device by the first web server;

a means for redirecting the web browser to the second web server by the first web server;

a means for sending the authentication token to the second web server by the web browser;

a means for decrypting the authentication token by the second web server;

a means for checking the pre-defined expiry of the authentication token by the second web server; and

a means for allowing the user to conduct a session with the second web server if within the pre-defined token expiry.

40. The system of claim 39 further comprising a means for allowing the user to conduct a session with the first web server.

41. The system of claim 40 wherein the second web server shares a sub-domain with the first web server.

42. The system of claim 41 wherein the means for digitally signing the authentication token by the first web server comprising means for digitally signing the authentication token using public key encryption.

43. The system of claim 42 further comprising a means for confirming a match with the digital signature.

44. A system of single sign-on for multiple web servers, comprising:

a means for receiving log-in data from a user in a first server;

a means for providing the user with a service selector;

a means for receiving an indication that the user selected the service selector;

a means for constructing an authentication token comprising profile data associated with the user;

a means for encrypting and signing the authentication token;

a means for redirecting the user to a second server;

a means for transmitting the authentication token to the user;

a means for receiving the authentication token in the second server;

a means for verifying the authentication token in the second server; and

a means for allowing the user access to a service provided by the second server.

45. The system of claim 44 wherein the authentication token further comprises expiration time data.

46. The system of claim 45 wherein the authentication token comprises a cookie.

47. The system of claim 46 wherein the log-in data comprises a user name and password.

48. The system of claim 47 wherein the service selector comprises a hyperlink.